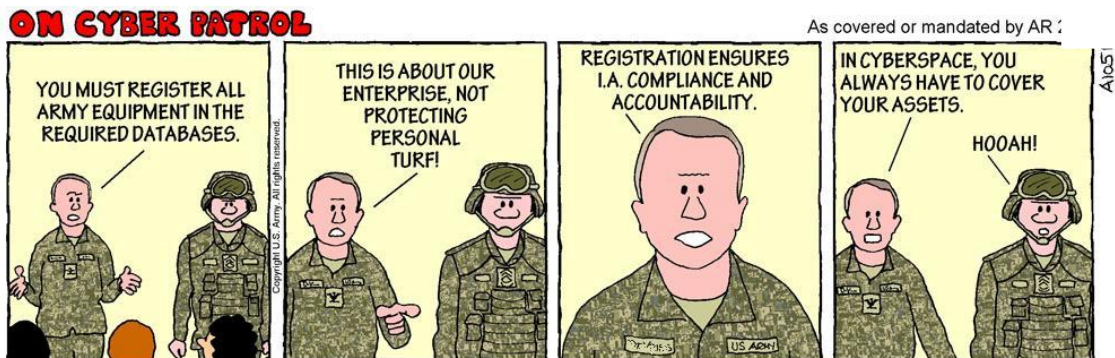


# An Argument for Asset Covering

April 2009



Securing the Enterprise does not mean locking down a starship, yet. But what does it mean? The “computer guys” know. But even they think about it in terms of boxes and wires or digital data. For the rest of us it means knowing where our computer “stuff” is and whether it is under physical and digital lock and key. It’s true that keeping track of all that “stuff” requires a lot of work. Some think it’s not worth the effort. Those who have fallen victim to a cyber attack or a breach of cyber security because of lost or unsecured assets would strongly disagree.

What does it take to enter your computer assets into an appropriate data base? Obviously, the answer is time and effort, two things in short supply. What do you get after taking the time and effort? On the surface, maybe not much. There’s no formal ceremony or high-fiving when the work is done. Job satisfaction? Maybe only for a few highly organized types. It’s just another administrative task that no one gets too excited about. Your work day doesn’t change. At the very least it’s another task crossed off your list. In fact, there’s a good chance you put it pretty far down your list.

What do you get if you don’t enter them into the database? A potential security breach because assets were unknowingly lost, stolen or because a critical security patch was not automatically installed. Then things get exciting.

We all do similar mundane tasks in our everyday lives. We keep financial records for tax purposes and balance our checkbooks. We collect and organize bills for timely payment. There are those who collect and organize store coupons. While that seems a waste of time and effort for some, others find the cash savings worth it, especially when the economy is bad.

The fact is that a great deal of administrative work goes into enabling the military to do its job. It also plays a major role in ensuring force protection. The tracking of computer assets is a critical task in our information assurance efforts. It’s the only way of keeping tabs on what we have, where it is, who is using it and how secure it is. That is a huge task when you think about how many computers and related pieces of hardware are out there. Yet we know that a smart, aggressive, opportunistic and hostile hacker can do a great deal of damage through just a single flaw in our cyber armor. That fact makes completing that task all the more important. Certainly the CIO of the Army thinks so, as do many of his fellow general officers and cyber security experts in all military branches and throughout the Federal government. Also, these experts make it clear that this critical task be performed from an Enterprise perspective. Local asset tracking alone does not create a unified, seamless, and secure network-centric enterprise environment.

In the big picture, tracking your computer assets protects missions and personnel. It also saves time and money due to the cost and effort of cleaning up after a cyber security breach. “Securing the Enterprise” is just a fancy name for covering our assets. In reality, it’s securing mission success and supporting the safety of the warfighter.